



SURVEILLANCE AND SECURITY CAMERA ACCEPTABLE USE POLICY

- Scope:** All campuses served by Louisiana State University (LSU) Police Department
- Effective:** January 2, 2020
- Procedures:** Departments requesting security cameras will be required to follow the procedures outlined in this policy regardless of funding source.

A. Purpose

Louisiana State University A&M Campus (“LSU” or the “University”) is committed to improving campus security, reducing risk, and enhancing the quality of life of the campus community, by integrating the best practices and tools of safety and security. A critical component of a comprehensive security plan is the utilization of an enterprise surveillance and security camera system that aligns IT, Police, and Facility concerns. The surveillance of public areas is intended to deter crime, support investigations, and assist in protecting the safety and property of the University. This policy addresses the university’s safety and security needs while respecting and preserving individual privacy.

The purpose of this policy is to regulate the use and management of camera systems used to observe and record public areas for the purposes of safety and security. To ensure the protection of individual privacy rights in accordance with the core values and state and federal laws, this policy is adopted to formalize procedures for the installation and maintenance of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records. The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

B. Definitions

- **Surveillance Cameras/Camera Systems:** Any camera or camera system operated with the intent of monitoring and/or influencing the behavior of people and protecting property.
- **Surveillance Oversight Committee (SOC):** An operational committee established by the Executive Vice President for Finance & Administration to oversee implementation of this policy.

C. General Policy

The Louisiana State University Police Department (LSUPD) has the authority to select, coordinate, operate, manage, and monitor all campus surveillance cameras and camera systems pursuant to this policy. All departments using camera surveillance are responsible for implementing and complying with this policy in their respective operations.

Upon initial Presidential approval of this policy, operators of noncompliant surveillance camera systems will receive notice of noncompliance and will have 12 calendar months from the date of notification to become compliant. Unapproved, unfunded, or nonconforming cameras will be removed from campus. Cameras are required to be compliant with the LSU Campus Design Standards. Departments with surveillance cameras are responsible for providing the funding necessary to bring their cameras into compliance.

Proposed policy revisions will be reviewed by the SOC, F&PO, and the IT Governance Council.

D. General Principles

Information obtained from surveillance cameras and camera systems shall be used for safety and security purposes, for incident documentation related to potential claims against the University, and for law and policy enforcement, including, where appropriate, student judicial functions. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure in accordance with PS 06.20: *Security of Data and/or Applicable Federal and State Laws*.

All appropriate measures must be taken to protect an individual's right to privacy and hold University information securely through its creation, storage, transmission, use, and deletion.

All surveillance camera installations are subject to federal and state laws.

Departments requesting surveillance cameras will be required to follow the procedures outlined in this policy.

E. Responsibilities

1. LSUPD, in conjunction with Information Technology Services (ITS) is responsible for the realization and assimilation of the policy provisions.

LSUPD and ITS are responsible for advising departments on appropriate applications of surveillance technologies and for providing technical assistance to departments preparing proposals for the purchase, installation, ongoing maintenance, and support of components of the University security camera system.

LSUPD and ITS shall monitor developments in the law and in security industry practices and technology to ensure that camera surveillance is consistent with the best practices and complies with all federal and state laws.

LSUPD, ITS, and the Office of Facility & Property Oversight (FPO) will review proposals and recommendations for camera installations and review specific camera locations to determine that the perimeter of view of fixed location cameras conform to this policy. Proposals for the installation of surveillance cameras shall be reviewed by the Chief of Police or designee. Recommendations shall be forwarded to the SOC. The SOC will consider requests from the Chief of Police and render a decision.

LSUPD, ITS, and F&PO will assess new camera locations, and will conduct an evaluation of existing camera locations.

Individual colleges, departments, programs, or campus organizations will be responsible for all costs related to purchase, installation, maintenance, removal, monitoring, storage, software, annual costs (if applicable) and network services (if necessary) for surveillance cameras not deemed essential for public safety or the management of risk by the SOC.

LSUPD will review any complaints regarding the utilization of surveillance camera systems, determine whether the terms of this policy are being followed, and either render a decision or refer the matter to the Office of Human Resource Management or other responsible unit. Appeals of a decision made by the Chief of Police will be made to and reviewed by the SOC which will make a recommendation to the Executive Vice President for Finance & Administration, who will render a decision. All decisions by the Executive Vice President for Finance & Administration on these matters are final.

2. Responsibilities of the Surveillance Oversight Committee (SOC)

The SOC will be responsible for reviewing and approving or denying all proposals for surveillance cameras/camera systems recommended by the Chief of Police. The SOC will review and approve any requested exceptions to this policy. The SOC shall propose to the Executive Vice President for Finance & Administration appropriate changes to this policy as needed.

The SOC shall be comprised of the following members:

- The Chief of Police or designee, Chair of the SOC
- Chief Technology Officer or designee
- Vice President for Student Affairs or designee
- Vice President for Legal Affairs and General Counsel or designee
- Associate Vice President for Facility and Property Oversight or designee
- Executive Director of Information Security, Risk and Emergency Management or designee

3. Responsibilities for Review of External Requests for Records Release

The LSUPD will review all external requests to release records obtained through security camera surveillance as part of their public safety responsibilities. The LSUPD must seek consultation and advice from the Office of General Counsel and other departments as deemed appropriate related to these requests prior to the release of any records.

F. Scope of Policy

This policy applies to all personnel, departments, colleges, and other units in the use of surveillance cameras and their video monitoring and recording systems, including but not limited to, any security cameras or video. Surveillance cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed campus-wide, inside, and outside buildings. Although the physical cameras may be identical, the functions of these cameras fall into four main categories:

- a) Property Protection: where the main intent is to capture video and store it on a remote device so that if property is reported stolen or damaged, the video may show the perpetrator. Examples: an unstaffed computer lab, an unstaffed science lab, or a parking lot.
- b) Personal Safety: where the main intent is to capture video and store it on a remote device so that if a person is assaulted or whose physical safety is otherwise negatively impacted or threatened, the video may capture the incident and the identity of persons involved. Examples of camera placement: a public walkway or a parking lot.
- c) Personal Security: where the main intent is to capture video and store it on a remote device to monitor access to secure entrance and exit points of a premise, the video may capture the unauthorized entry and person involved. Examples of camera placement: Interior and exterior card access operated doors in residential areas.
- d) Extended Responsibility: where the main intent is to have the live video stream in one area monitored by a staff member in close proximity. Example: a single staff monitoring multiple entry and exit parts of a building.

G. Placement of Cameras

The locations where cameras are installed may be restricted access sites such as departmental computer lab; however, an individual does not have a reasonable expectation of privacy at these types of locations. Cameras will be located so that personal privacy is maximized.

No audio shall be recorded. Requests to utilize audio surveillance will be evaluated on a case-by-case basis by the SOC and Office of the General Counsel.

Camera positions and views of residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

Unless the camera is being used for criminal investigations, installation of and/or monitoring by surveillance cameras in the following locations is prohibited:

- Student rooms in the residence halls
- Restrooms
- Shower facilities
- Locker rooms
- Offices

The installation of “dummy” cameras that do not operate is prohibited.

Unless being used for criminal investigations, all surveillance camera installations should be visible.

H. Access and Monitoring

All recording or monitoring of activities of individuals or groups by University security cameras is considered confidential information and will be conducted and accessed in a manner consistent with University policies, state and federal laws, and will not be based on subjects’ personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics. Any access of recordings for assessing job related issues must have prior approval of the Office of Human Resource Management.

University security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Chief of Police or designee.

For Property Protection, Personal Safety, and Personal Security (as defined in the Scope above) access to live video or recorded video from cameras shall be limited to authorized personnel of the department which installed the cameras, LSUPD, and other persons authorized by the Chief of Police or designee. The copying, duplicating, and/or retransmission of live or recorded video shall be limited to persons authorized by the Chief of Police or designee.

Nothing in this section is intended to limit the authority of the LSUPD in law enforcement activities.

I. Appropriate Use and Confidentiality

Personnel are prohibited from using or disseminating information acquired from university security cameras. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official University and law enforcement purposes. Personnel are expected to know and follow University Policies PS 107, Computer Users’ Responsibilities, and PS 06.25, Privacy of Computing Resources.

J. Use of Cameras for Criminal Investigations

The use of mobile or hidden video equipment may be used in criminal investigations by the LSUPD. Covert video equipment may also be used for non-criminal investigations of specific instances which may be a significant risk to public safety, security and property as authorized by the Chief of Police or designee.

K. Exceptions

This policy does not apply to cameras used for academic purposes. Cameras that are used for research are governed by other policies involving human subjects and are therefore excluded from this policy.

This policy does not address the use of webcams for the general use by the University (e.g., on the official LSU website). This policy also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Such cameras and video footage are not considered “surveillance” for the purposes of this policy, thus falling outside the scope of this policy. Examples of such excluded activities include videotaping

of athletic events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are exempt from this policy.

Also excluded are security cameras installed and operated on the interior of premises which LSU has leased to others, such as the Nicholson Gateway retailers, the CAA animal shelter, etc.

Even though excluded, all cameras installed must be readily compliant with data and management system standards set forth by the University.

L. Training

Camera control operators shall receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.

M. Storage and Retention of Recordings

No attempt shall be made to alter any part of any surveillance recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

All surveillance records shall be stored in a centralized, secure University location for a minimum period of 15 days and will then promptly be erased or recorded over, unless retained as part of a criminal investigation, for incident documentation related to potential claims against the University, or court proceedings (criminal or civil), or other bona fide use as approved by the Chief of Police or designee. Individual departments shall not store video surveillance recordings.